REMARKS / ARGUMENTS

The present application includes pending claims 1-34, all of which have been rejected. Claims 3-5, 13-15 and 23-25 were objected to. By this Amendment, claims 3,4, 6-10, 13, 14, 16-20, 23, 24 26-29, 32 and 33 have been amended, as set forth above, to further clarify the language used in these claims and to further prosecution of the present application. The Applicant respectfully submits that the claims define patentable subject matter.

Initially, the Applicant notes that a goal of patent examination is to provide a prompt and complete examination of a patent application.

> It is essential that patent applicants obtain a prompt yet complete examination of their applications. Under the principles of compact prosecution, each claim should be reviewed for compliance with every statutory requirement for patentability in the *initial review* of the application, even if one or more claims are found to be deficient with respect to some statutory requirement. Thus, Office personnel *should* state *all* reasons and bases for rejecting claims in the *first* Office action. Deficiencies should be explained clearly, particularly when they serve as a basis for a rejection. Whenever practicable, Office personnel should indicate how rejections may be overcome and how problems may be resolved. A failure to follow this approach can lead to unnecessary delays in the prosecution of the application.

See Manual of Patent Examining Procedure (MPEP) § 2106(II). As such, the Applicant assumes, based on the goals of patent examination noted above, that the present Office Action has set forth "all reasons and bases" for rejecting the claims.

Claims 3-5, 13-15 and 23 - 25 were objected to because the claim language was considered to be ambiguous by the Examiner. Claims 1, 2, 6, 10-12, 16, 20-22, 26, and 30-31 stand rejected under 35 U.S.C. § 102(e) as being anticipated by US Patent Publication No. 2003/0007644, by Sprunk et al. (hereinafter, Sprunk et al.). Claims 3-5, 13-15 and 23-25 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Sprunk et al., in view of "Applied Cryptography", 2nd Edition, 1996 by Schneier (hereinafter, Schneier). Claims 7-9, 17-19 and 27-29 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Sprunk et al., in view of US Patent 4,864,615, issued to Bennett et al. (hereinafter, Bennett et al.). Claims 32-34 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Sprunk et al., in view of US Patent 7,028,014, issued to Naclerio. (hereinafter, Naclerio).

The Applicant respectfully traverses these objections and rejections at least for the reasons previously set forth during prosecution and at least based on the following remarks.

CLAIM OBJECTIONS

Claims 3-5, 13-15 and 23 - 25 were objected to because the claim language "equivalent to" was considered to be ambiguous by the Examiner. The Applicant has amended claim 3, 4, 13, 14, 23, and 24 as set forth above to overcome this

rejection. Claims 5, 15 and 25 do not contain the objected expression but depend on claims 4, 14 and 24, respectively. In view of the amendment to claims 3, 4, 13, 14, 23, and 24, the Applicant respectfully submits that the objection to claims 3-5, 13-15 and 23 - 25 be withdrawn and the claims made allowable.

REJECTION UNDER 35 U.S.C. § 102

I. Sprunk et al. Does Not Anticipate Claims 1, 2, 6, 10-12, 16, 20-22, 26, and 30-31

The Applicant first turns to the rejection of claims **1, 2, 6, 10-12, 16, 20-22, 26, and 30-31** under 35 U.S.C. 102(e) as being anticipated by Sprunk et al.. With regard to the anticipation rejections under 102(e), MPEP 2131 states that "[a] claim is anticipated only if **each and every element** as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." See Manual of Patent Examining Procedure (MPEP) at 2131 (internal citation omitted). Furthermore, "[t]he identical invention must be shown in as complete detail as is contained in the ... claim." See id. (internal citation omitted).

A. Rejection of Independent Claims 1, 11 and 21 under 35 U.S.C. § 102(e)

With regard to the rejection of independent claim 1 under 35 U.S.C. §102(e), the Applicant submits that Sprunk et al. does not disclose or suggest at least the limitation of "receiving at least a first input key, a second input key and a third input key," as recited by the Applicant in independent claim 1. More specifically, Sprunk et al does not teach that an initialization vector (IV) is a key, as argued by the examiner. The Office Action refers for support to Figure 4 and paragraph [0036] of Sprunk et al. and the examiner states that "... and the IV (Initial Value) is considered as one of key variation values and is qualified as a third input key". Paragraph [0036], however, does not support the examiners opinion that the IV is equal to a key.

DES (Data Encryption Standard), as cited in the passage referred to by the examiner in paragraph [0036], is standardized by the National Institute of Standards and Technology (NIST) and published in the Federal Information Processing Standards Publications (FIPS PUBS). The Applicant points out that FIPS PUB 81, which is one of the relevant standards for DES, entitled "DES Modes of Operation", published on December 2, 1980, defines "Initialization Vector" as follows:

> INITIALIZATION VECTOR (IV): A binary vector used in the initial input block in the CFB and OFB modes and

> as the randomizing block that is exclusive- ORed with the first data block in the CBC mode.

where the abbreviation CFB stands for 'cipher feedback', OFB stands for 'output feedback' and CBC stands for 'cipher block chaining', as defined in FIPS PUBS 81. The Applicant notes that the definition of "Initialization Vector" makes no reference to the Initialization Vector being a key.

Furthermore, there is no indication in either Figure 4 or paragraph [0036] of Sprunk et al. of that an IV may be "received". Since neither receiving an IV nor that an IV is equal to a key is disclosed, taught or suggested in the passages cited in the Office Action of Sprunk et al., the applicant submits that claim 1 be made allowable and the rejection withdrawn.

Furthermore, the Applicant submits that Sprunk et al. does not disclose:

> generating a first output key based on said at least said first input key, said second input key and said third input key, wherein said first output key is unique and differs from said at least said first input key

as recited by the Applicant. For example, Sprunk et al. does not teach "said output key is unique". The Office action argues that "Sprunk teaches the desirable output key should not be repeated (Para [0017] Line 4-5)". The text segment quoted by the Examiner states:

> This is desirable since keys should not be repeated, and a large number of unused keys should always remain.

The cited passage does, however, not teach "output key". Furthermore, "keys should not be repeated" implies that it is possible or desirable that keys are not

repeated. This does not, however, imply uniqueness as recited by the applicant in "said output key is unique". Therefore, the Applicant submits that "said output key is unique" is not taught by Sprunk et al. and respectfully submits that claim 1 be made allowable and the rejection under 35 U.S.C. §102(e) be withdrawn.

Accordingly, independent claim 1 is not anticipated by Sprunk et al. and is allowable. Independent claims 11 and 21 are similar in many respect to the method disclosed in independent claim 1. Therefore, the Applicant submits that independent claims 11 and 21 are also allowable over the references cited in the Office Action at least for the reasons stated above with regard to claim 1.

B. Rejection of Dependent Claims 2, 6, 10, 12, 16, 20, 22, 26, 30 and 31

Based on at least the foregoing, the Applicant believes the rejection of independent claims 1, 11 and 21 under 35 U.S.C. § 102(e) as being anticipated by Sprunk et al. has been overcome and request that the rejection be withdrawn. Additionally, claims 2, 6, 10, 12, 16, 20, 22, 26, 30 and 31 depend from independent claims 1, 11 and 21, respectively, and are, consequently, also respectfully submitted to be allowable.

Applicant also reserves the right to argue additional reasons beyond those set forth above to support the allowability of claims 1, 2, 6, 10-12, 16, 20-22, 26, and 30-31.

REJECTION UNDER 35 U.S.C. § 103

Claims 3-5, 13-15 and 23-25 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Sprunk et al., in view of "Applied Cryptography", 2nd Edition, 1996 by Schneier. Claims 7-9, 17-19 and 27-29 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Sprunk et al., in view of Bennett et al. Claims 32-34 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Sprunk et al., in view of Naclerio.

The Applicant notes that all rejections under 35 U.S.C. §103(a) are rejections of dependent claims that depend on independent claims 1, 11 and 21. Since the independent claims 1, 11 and 21 have not been objected to and are believed to be allowable, the Applicant submits that the rejection of dependent claims 3-5, 13-15, 23-25, 7-9, 17-19, 27-29 and 32-34 under 35 U.S.C. §103(a) be withdrawn and the claim be made allowable.

CONCLUSION

Based on at least the foregoing, the Applicant believes that all claims 1-34 are in condition for allowance. If the Examiner disagrees, the Applicant respectfully requests a telephone interview, and request that the Examiner telephone the undersigned Attorney at (312) 775-8176.

The Commissioner is hereby authorized to charge any additional fees or credit any overpayment to the deposit account of McAndrews, Held & Malloy, Ltd., Account No. 13-0017.

A Notice of Allowability is courteously solicited.

Respectfully submitted,

Date: June 4, 2007

/Ognyan I. Beremski/

Ognyan I. Beremski, Esq.
Registration No. 51,458
Attorney for Applicant

McAndrews, Held & Malloy, Ltd.
500 West Madison Street, 34th Floor
Chicago, Illinois 60661
(312) 775-8000

/ OIB